

1. An unauthorized-alteration detecting method comprising:

5 a step in which a processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

10 a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained by block-dividing an original image $[f]$ to which embedding is to be applied;

15 a step in which the processing section uses the modulus P , the order N , and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;

a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

20 a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to be embedded;

25 a step in which the processing section obtains an embedding amount δ in each block from the number-theoretic-transformed block $F_{i,j}(x', y')$ of the original-image block at the embedding position, the pixel value $g_{i,j}$ of the signature image, and embedding strength ϵ ;

30 a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block, based on (x, y) to obtain the number-theoretic-transformed block $H_{i,j}(x, y)$ of an embedding-applied-image block;

REF ID: A62854
APR 1967

a step in which the processing section applies inverse number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-image block $h_{i,j}(x, y)$; and

5 a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage section and/or outputs it from an output section or an
10 interface.

2. An unauthorized-alteration detecting method comprising:

a step in which a processing section reads from a storage section, an input section, or an interface an
15 embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-dividing an embedding-applied image $[h]$;

a step in which the processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

20 a step in which the processing section applies the number theoretic transform to the embedding-applied-image block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image block;

25 a step in which the processing section determines an extraction position (x', y') corresponding to an embedding position of a signature image according to a predetermined randomizing function;

a step in which the processing section obtains a
30 remainder by dividing the number-theoretic-transformed block $H_{i,j}(x', y')$ at the extraction position by embedding strength ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j) blocks or a desired range of (i, j) blocks to obtain the signature image $[g]$, and stores it in the storage section and/or outputs it from a display section, an output section, or an interface.

3. An unauthorized-alteration detecting method comprising an embedding process for embedding a signature image into an original image and an extraction process for extracting the signature image,

wherein the embedding process comprises:

a step in which a processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained by block-dividing an original image $[f]$ to which embedding is to be applied;

a step in which the processing section uses the modulus P , the order N , and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;

a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to be embedded;

a step in which the processing section obtains an embedding amount δ in each block from the number-theoretic-

transformed block $F_{i,j}(x', y')$ of the original-image block at the embedding position, the pixel value $g_{i,j}$ of the signature image, and embedding strength ε ;

a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block, based on (x, y) to obtain the number-theoretic-transformed block $H_{i,j}(x, y)$ of an embedding-applied-image block;

a step in which the processing section applies inverse number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-image block $h_{i,j}(x, y)$; and

a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage section and/or outputs it from an output section or an interface,

and

the extraction process comprises:

a step in which the processing section reads from the storage section, the input section, or the interface an embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-dividing an embedding-applied image $[h]$;

a step in which the processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section applies the number theoretic transform to the embedding-applied-image block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image

REPLACED BY
AUTOMATIC

block;

a step in which the processing section determines an extraction position (x', y') corresponding to an embedding position of a signature image according to a predetermined

5 randomizing function;

a step in which the processing section obtains a remainder by dividing the number-theoretic-transformed block $H_{i,j}(x', y')$ at the extraction position by embedding strength ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

10 a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j) blocks or a desired range of (i, j) blocks to obtain the signature image $[g]$, and stores it in the storage section and/or outputs it from a display section, the output section,
15 or the interface.

4. An unauthorized-alteration detecting method according to Claim 1 or 3, further comprising a step in which the processing section transmits the modulus P and the
20 embedding-applied image $[h]$, and, if necessary, the order N to an extraction-side apparatus through the output section or the interface.

5. An unauthorized-alteration detecting method according to
25 Claim 2 or 3, further comprising a step in which the processing section receives the modulus P , which is a parameter of the number theoretic transform, and the embedding-applied image $[h]$, and, if necessary, the order N from a transmission-side apparatus.

30

6. An unauthorized-alteration detecting method according to one of Claims 1 to 3, further comprising a step in which the

processing section obtains the original image [f] according to the embedding-applied image [h] and the signature image [g].

5 7. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein P is any compound number generated by a power of a prime number.

10 8. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein N is common to an embedding side and an extraction side of the signature image and stored in advance in the storage section, or is transferred from the embedding side to the extraction side.

15 9. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein the processing section selects the order N among candidates of the order N, obtained by $N | \text{GCD}[(p_1 - 1), (p_2 - 1), \dots, (p_m - 1)]$ according to a predetermined priority.

20 10. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein the processing section calculates the root α uniquely determined according to a predetermined expression of the Chinese remainder theorem or
25 others, based on the modulus P and the order N specified.

11. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein

the processing section specifies P expressed by $P = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$, where p_1 is a prime number and r_1 is a positive
30 integer;

the processing section selects the order N among

positive integers satisfying $N | \text{GCD}[(p_1 - 1), (p_2 - 1), \dots, (p_m - 1)]$, or reads the order N from the storage section;

the processing section calculates a root $\alpha_{1,1}$ of the order N with respect to the modulus p_1 ;

5 the processing section obtains a root $\alpha_{2,1}$ of the order N with respect to the modulus $p_1^{r_1}$ from $\alpha_{1,1}$; and

the processing section obtains the root α of the order N with respect to the modulus P from $\alpha_{2,1}$ according to the Chinese remainder theorem.

10

12. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein the processing section uses P , N , and α to execute the number theoretic transform between $x(n)$ and $X(k)$ by the following expressions,

$$X(k) = \sum_{n=0}^{N-1} x(n) \alpha^{kn} \pmod{P} \quad (1)$$

$$x(n) = N^{-1} \sum_{k=0}^{N-1} X(k) \alpha^{-kn} \pmod{P} \quad (2)$$

15

wherein P is any compound number generated by a power of a prime number, α is a positive integer, N is the minimum positive integer satisfying $\alpha^N = 1 \pmod{P}$,

$$X = [T]x$$

20 $x = [T]^{-1}X$

$[T]$ is a transformation matrix, and $[T]^{-1}$ is an inverse transformation matrix.

13. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein the randomizing function uses the value of the modulus P and/or a pixel value in an adjacent block or a pixel value in a predetermined block which is not changed by an embedding process, as a parameter,

25

and determines the position uniquely.

14. An unauthorized-alteration detecting method according to one of Claims 1 to 3, wherein the randomizing function is
5 specified by the following expressions.

$$x' = r_{x'}(P, i, j, f_{i,l}(0, 0)) \quad (10)$$

$$y' = r_{y'}(P, i, j, f_{i,l}(0, 0)) \quad (11)$$

$$l = j - 1 \pmod{L} \quad (12)$$

15. An unauthorized-alteration detecting program for making a computer execute each of the following steps, the
10 following steps including:

a step in which a processing section specifies a modulus P, an order N, and a root α , which are parameters of number theoretic transform;

- 15 a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained by block-dividing an original image [f] to which embedding is to be applied;

- 20 a step in which the processing section uses the modulus P, the order N, and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;

- 25 a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to be embedded;

a step in which the processing section obtains an

EXCLUDED BY
ADVISORY

embedding amount δ in each block from the number-theoretic-transformed block $F_{i,j}(x', y')$ of the original-image block at the embedding position, the pixel value $g_{i,j}$ of the signature image, and embedding strength ε ;

5 a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block, based on (x, y) to obtain the number-theoretic-transformed block $H_{i,j}(x, y)$ of an embedding-applied-image
10 block;

 a step in which the processing section applies inverse number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-image block $h_{i,j}(x, y)$; and

15 a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage section and/or outputs it from an output section or an
20 interface.

16. An unauthorized-alteration detecting program for making a computer execute each of the following steps, the following steps including:

25 a step in which a processing section reads from a storage section, an input section, or an interface an embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-dividing an embedding-applied image $[h]$;

 a step in which the processing section specifies a
30 modulus P , an order N , and a root α , which are parameters of number theoretic transform;

 a step in which the processing section applies the

number theoretic transform to the embedding-applied-image block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image block;

5 a step in which the processing section determines an extraction position (x', y') corresponding to an embedding position of a signature image according to a predetermined randomizing function;

10 a step in which the processing section obtains a remainder by dividing the number-theoretic-transformed block $H_{i,j}(x', y')$ at the extraction position by embedding strength ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

15 a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j) blocks or a desired range of (i, j) blocks to obtain the signature image $[g]$, and stores it in the storage section and/or outputs it from a display section, an output section, or an interface.

20 17. An unauthorized-alteration detecting program for making a computer execute an embedding process for embedding a signature image into an original image and an extraction process for extracting the signature image,

wherein the embedding process comprises:

25 a step in which a processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

30 a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained by block-dividing an original image $[f]$ to which embedding is to be applied;

 a step in which the processing section uses the modulus

P, the order N, and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;

5 a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

 a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to
10 be embedded;

 a step in which the processing section obtains an embedding amount δ in each block from the number-theoretic-transformed block $F_{i,j}(x', y')$ of the original-image block at the embedding position, the pixel value $g_{i,j}$ of the signature
15 image, and embedding strength ε ;

 a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block, based on (x, y) to obtain the number-theoretic-
20 transformed block $H_{i,j}(x, y)$ of an embedding-applied-image block;

 a step in which the processing section applies inverse number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-
25 image block $h_{i,j}(x, y)$; and

 a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage
30 section and/or outputs it from an output section or an interface,

and

REPLACED BY
AN 91/MDT

the extraction process comprises:

a step in which the processing section reads from the storage section, the input section, or the interface an embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-
5 dividing an embedding-applied image [h];

a step in which the processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section applies the
10 number theoretic transform to the embedding-applied-image block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image block;

a step in which the processing section determines an
15 extraction position (x', y') corresponding to an embedding position of a signature image according to a predetermined randomizing function;

a step in which the processing section obtains a remainder by dividing the number-theoretic-transformed block
20 $H_{i,j}(x', y')$ at the extraction position by embedding strength ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j) blocks or a desired range of (i, j) blocks to obtain the
25 signature image [g], and stores it in the storage section and/or outputs it from a display section, the output section, or the interface.

18. A recording medium having recorded an unauthorized-
30 alteration detecting program for making a computer execute each of the following steps, the following steps including:

a step in which a processing section specifies a

modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained
5 by block-dividing an original image $[f]$ to which embedding is to be applied;

a step in which the processing section uses the modulus P , the order N , and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;
10

a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

15 a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to be embedded;

a step in which the processing section obtains an embedding amount δ in each block from the number-theoretic-transformed block $F_{i,j}(x', y')$ of the original-image block at
20 the embedding position, the pixel value $g_{i,j}$ of the signature image, and embedding strength ϵ ;

a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image
25 block, based on (x, y) to obtain the number-theoretic-transformed block $H_{i,j}(x, y)$ of an embedding-applied-image block;

a step in which the processing section applies inverse
30 number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-image block $h_{i,j}(x, y)$; and

a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage
5 section and/or outputs it from an output section or an interface.

19. A recording medium having recorded an unauthorized-alteration detecting program for making a computer execute
10 each of the following steps, the following steps including:

a step in which a processing section reads from a storage section, an input section, or an interface an embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-dividing an embedding-applied image $[h]$;

15 a step in which the processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section applies the number theoretic transform to the embedding-applied-image
20 block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image block;

a step in which the processing section determines an extraction position (x', y') corresponding to an embedding
25 position of a signature image according to a predetermined randomizing function;

a step in which the processing section obtains a remainder by dividing the number-theoretic-transformed block $H_{i,j}(x', y')$ at the extraction position by embedding strength
30 ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j)

blocks or a desired range of (i, j) blocks to obtain the signature image [g], and stores it in the storage section and/or outputs it from a display section, an output section, or an interface.

5

20. A recording medium having recorded an unauthorized-alteration detecting program for making a computer execute an embedding process for embedding a signature image into an original image and an extraction process for extracting the signature image,

wherein the embedding process comprises:

a step in which a processing section specifies a modulus P, an order N, and a root α , which are parameters of number theoretic transform;

15 a step in which the processing section reads from a storage section an original-image block $f_{i,j}(x, y)$ obtained by block-dividing an original image [f] to which embedding is to be applied;

a step in which the processing section uses the modulus P, the order N, and the root α specified, to apply the number theoretic transform to the original-image block $f_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block;

25 a step in which the processing section determines an embedding position (x', y') of a signature image in each block according to a predetermined randomizing function;

a step in which the processing section reads from the storage section a pixel value $g_{i,j}$ of the signature image to be embedded;

30 a step in which the processing section obtains an embedding amount δ in each block from the number-theoretic-transformed block $F_{i,j}(x', y')$ of the original-image block at

the embedding position, the pixel value $g_{i,j}$ of the signature image, and embedding strength ε ;

a step in which the processing section adds or subtracts the embedding amount δ to or from the number-theoretic-transformed block $F_{i,j}(x, y)$ of the original-image block, based on (x, y) to obtain the number-theoretic-transformed block $H_{i,j}(x, y)$ of an embedding-applied-image block;

a step in which the processing section applies inverse number theoretic transform to the number-theoretic-transformed block $H_{i,j}(x, y)$ to obtain the embedding-applied-image block $h_{i,j}(x, y)$; and

a step in which the processing section obtains the embedding-applied-image block $h_{i,j}(x, y)$ for each of all (i, j) blocks or a desired range of (i, j) blocks to obtain an embedding-applied image $[h]$, and stores it in the storage section and/or outputs it from an output section or an interface,

and

the extraction process comprises:

a step in which the processing section reads from the storage section, the input section, or the interface an embedding-applied-image block $h_{i,j}(x, y)$ obtained by block-dividing an embedding-applied image $[h]$;

a step in which the processing section specifies a modulus P , an order N , and a root α , which are parameters of number theoretic transform;

a step in which the processing section applies the number theoretic transform to the embedding-applied-image block $h_{i,j}(x, y)$ to calculate the number-theoretic-transformed block $H_{i,j}(x, y)$ of the embedding-applied-image block;

a step in which the processing section determines an extraction position (x', y') corresponding to an embedding position of a signature image according to a predetermined randomizing function;

5 a step in which the processing section obtains a remainder by dividing the number-theoretic-transformed block $H_{i,j}(x', y')$ at the extraction position by embedding strength ϵ to extract a pixel value $g_{i,j}$ of the signature image; and

10 a step in which the processing section obtains the pixel value $g_{i,j}$ of the signature image in each of all (i, j) blocks or a desired range of (i, j) blocks to obtain the signature image $[g]$, and stores it in the storage section and/or outputs it from a display section, the output section, or the interface.